REMARKS

Applicants appreciate the thorough examination as reflected in the Official Action mailed April 23, 2002. Applicants also appreciate the indication of allowable subject matter in Claims 6-8, 19-21 and 32-34. Various claims have been amended herein to correct typographic errors that were noted upon review. These amendments are merely typographical and do not impact the scope of the claims or the range of equivalents thereto.

The Section 101 Rejections

Claims 1, 14, 27, 40, 46 and 52 stand rejected under 35 U.S.C. § 101 as directed to non-statutory subject matter. In particular, the Official Action states that the claimed invention "fails to define a useful tangible result with regards to the specific information and the entity specific information." Official Action, p. 2.

Applicants respectfully submit that Claims 1, 14, 27, 40, 46 and 52 define a useful tangible result. For example, Claim 1 recites selecting an RSA prime. As discussed in the background section of the present application, an RSA prime is used in the derivation of RSA public and private keys. Specification, p. 2, lines 14-28. Thus, Claim 1 provides a useful, tangible result in the selection of an RSA prime value that may be used for RSA key generation. Similar recitations are found in Claims 14 and 27. Thus, Claims 14 and 27 also provide systems and computer program products that provide tangible, useful results.

Claims 40, 46 and 52 each recite "selecting a cryptographic value" and, therefore, also provide a tangible useful result in that a cryptographic value corresponding to a source entity is selected for use in further cryptographic processing. Accordingly, Applicants respectfully submit that Claims 40, 46 and 52 also meet the statutory requirements of Section 101.

Applicants also note that the Austin reference cited in the Official Action has claims directed to "a method of generating key values." Thus, it appears that the Patent Office has previously considered claims directed to generating cryptographic values as including statutory subject matter.

With regard to Claims 40-43 and 46-49, Applicants submit that these claims meet the requirements of Section 101 as they depend from a claim that meets those requirements.

The Section 102 Rejections

Claims 1-5, 9, 14-18, 22, 27-31, 35, 40, 44-46, 50-52, 56 and 57 stand rejected under 35 U.S.C. § 102(b) as anticipated by United States Patent No. 4,944,007 to Austin (hereinafter "Austin"). In particular, the Official Action cites to Figure 3 of Austin as disclosing each of the recitations of Claims 1-5, 9, 14-18, 22, 27-31, 35, 40, 44-46, 50-52, 56 and 57. Claims 1, 14, 27, 40, 46 and 52 are independent claims. Claims 14 and 27 are system and computer program product claims having recitations corresponding to Claim 1. Claims 46 and 52 are system and computer program product claims having recitations corresponding to Claim 40. Thus, Applicants will address the rejections with reference to Claims 1 and 40, however, analogous arguments apply with respect to Claims 14, 27, 46 and 52. Applicants will first address the rejections of the independent claims and then address the rejections of the dependent claims.

Claim 1 of the present application recites:

> 1. A method of generating an RSA cryptographic value, the method comprising the steps of:
>
> obtaining user specific information about a user;
>
> dividing a potential range of RSA prime values into at least two subintervals; and
>
> selecting a first user-dependent RSA prime from a range of RSA prime values in a first of the at least two subintervals corresponding to a user specific range of values based on the user specific information mapped onto the first subinterval.

Thus, Claim 1 recites at least two subintervals where an RSA prime value is selected from a range of prime values in a first of the two subintervals. The range from which the RSA prime value is selected corresponds to a user specific range of values that is based on user specific information and that is mapped onto the first subinterval. Such a mapping is illustrated, for example, in Figure 5 of the present application that is reproduced below.

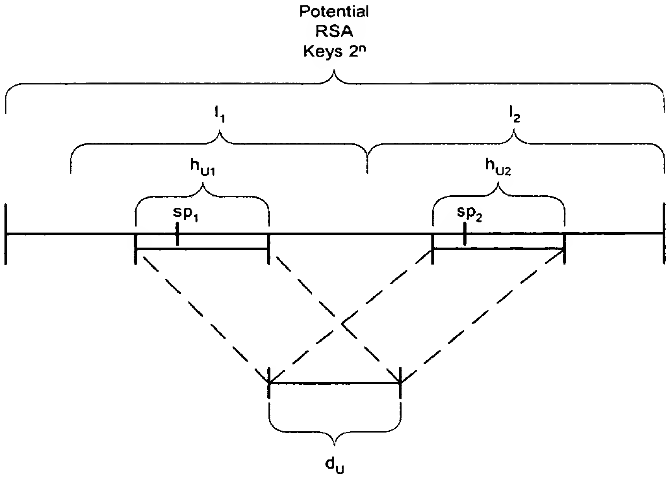

Figure 5

As seen in Figure 5, the range of values that are based on user specific information (d_u) is mapped onto the subinterval I_1 to provide the range h_{u1} within the subinterval I_1. The RSA prime value sp_1 is then selected from the range h_{u1}. Such a mapping of a user dependent range is recited in Claim 1 as "selecting a first user-dependent RSA prime," e.g. sp_1, "from a range of RSA prime values in a first of the at least two subintervals," e.g. h_{u1}, "corresponding to a user specific range of values," e.g. d_u, "based on the user specific information mapped onto the first subinterval."

Claim 14, likewise, recites:

> 14. A system for generating an RSA cryptographic value, comprising:
>
> means for obtaining user specific information about a user; and
>
> means for determining a user specific range of values based on the user specific information;
>
> means for dividing a potential range of RSA prime values into at least two subintervals;
>
> means for mapping the user specific range of values onto a first of the at least two subintervals; and
>
> means for selecting a first user-dependent RSA prime from the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values.

Similar recitations are found in Claim 27. Thus, Claims 14 and 27 recite the mapping of a user specific range of values onto a subinterval and selection of an RSA prime from that subinterval. Applicants submit that the recitations of Claims 1, 14 and 27 are not disclosed or suggested by Austin for the reasons discussed below.

In particular, it appears that Austin only uses the member ID as a tag or identifier of stored values. Austin, col. 6, lines 5-7. While Austin does indicate that values for T and U are selected from a range of values that differs from the range that includes P, Q, R and S, Austin does not describe the range of values based on user dependent information or that the range of values from which T and U are selected corresponds to the user dependent range of values mapped onto a subinterval. See Austin, col. 6, lines 49-60. Accordingly, Applicants submit that the recitations of Claim 1 are not disclosed or suggested by Austin.

Claims 14 and 27 expressly recite "determining a user specific range of values based on the user specific information" and "mapping the user specific range of values onto a first of the at least two subintervals." Applicants submit that if the boundary between where P, Q, R and S are selected and where T and U are selected in Austin is considered dividing the range into two subintervals then Austin does not disclose or suggest the determination of a user specific range and mapping that range onto the two subintervals. Thus "member ID" of Austin is not used in the selection of values but is used as an identification when the values are stored. Accordingly, Applicants submit that Austin does not disclose or suggest each of the recitations of Claims 14 and 27.

Austin is also cited as disclosing each of the recitations of independent claims 40, 46 and 52. Claims 40, 46 and 52 provide for selecting cryptographic ranges that are different for different entities. For example, Claim 40 recites:

> 40. (Original) A method of generating a cryptographic value corresponding to a source entity, the method comprising the steps of:
>
> obtaining entity specific information associated with the source entity; and
>
> selecting a cryptographic value from a range of cryptographic values based on the entity specific information, wherein the range of cryptographic values based on the entity specific information is disjoint with ranges of cryptographic values associated with entity specific information associated with entities other than the source entity.

Similar recitations are found in Claims 46 and 52. Applicants respectfully submit that the recitations of Claims 40, 46 and 52 are not disclosed or suggested by Austin.

While at col. 6, lines 49-60, Austin does describe two separate ranges between primes generated by the parent and primes generated by a member, Austin does not describe the ranges as being disjoint between all members and the parent processor. Thus, Applicants submit that Austin does not disclose or suggest "the range of cryptographic values based on the entity specific information is disjoint with ranges of cryptographic values associated with entity specific information associated with entities other than the source entity." Accordingly, Applicants submit that each of the recitations of Claims 40, 46 and 52 are not disclosed or suggested by Austin.

With regard to the dependent claims, Applicants submit that the dependent claims are patentable as depending from a patentable base claim. However, certain of the dependent claims are also separately patentable over Austin. For example, Claim 2 recites "selecting a second user-dependent RSA prime from a range of RSA prime values in a second of the at least two subintervals, different from the first subinterval, corresponding to the user specific range of values based on the user specific information mapped onto the second subinterval." Claims 15 and 28 recite "means for mapping the user specific range of values onto a second of the at least two subintervals, different from the first of the at least two subintervals" and "means for selecting a second user-dependent RSA prime from the range of RSA prime values in the second of the at least two subintervals corresponding to the mapped user specific range of values." Applicants submit that selection of RSA prime values from two different subintervals where the range from which the primes are selected is based on a mapping of a user specific range to the subintervals is not disclosed or suggested by the cited portions of Austin. Accordingly, Applicants submit that Claims 2, 15 and 28 are separately patentable for at least these additional reasons.

Claims 3, 16 and 29 recite that the user specific range values are mapped linearly onto the first subinterval. Applicants submit that such a linear mapping is not disclosed or suggested by the cited portions of Austin. Accordingly, Applicants submit that Claims 3, 16 and 29 are separately patentable for at least these additional reasons.

Claims 4, 17 and 30 recite that the same mapping function is used to map the user specific range of values onto the first subinterval and onto the second subinterval. Applicants submit that use of the same mapping function to map a user specific range of values onto two different subintervals is not disclosed or suggested by Austin. Accordingly, Applicants submit that Claims 4, 17 and 30 are separately patentable for at least these additional reasons.

In light of the above discussion, Applicants respectfully submit that Claims 1-5, 9, 14-18, 22, 27-31, 35, 40, 44-46, 50-52, 56 and 57 are not anticipated by Austin.

The Section 103 Rejections

Claims 10, 11, 23, 24, 36, 37, 41, 42, 47, 48, 53 and 54 stand rejected as obvious under 35 U.S.C. § 103 based on the combination of Austin and United States Patent No. 5,680,460 to Tomko *et al.* (hereinafter "Tomko"). Applicants submit that each of Claims 10, 11, 23, 24, 36, 37, 41, 42, 47, 48, 53 and 54 are patentable as depending from a patentable base claim.

Claims 12, 13, 25, 26, 38 and 39 stand rejected as obvious under 35 U.S.C. § 103 based on the combination of Austin and United States Patent No. 6,226,383 to Jablon (hereinafter "Jablon"). Applicants submit that each of Claims 12, 13, 25, 26, 38 and 39 are patentable as depending from a patentable base claim.

Claims 43, 49 and 55 stand rejected as obvious under 35 U.S.C. § 103 based on the combination of Austin and United States Patent No. 5,709,114 to Dawson *et al.* (hereinafter "Dawson"). Applicants submit that each of Claims 43, 49 and 55 are patentable as depending from a patentable base claim.

Conclusion

In light of the above discussion, Applicant submits that the present application is in condition for allowance, which action is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

It is not believed that an extension of time and/or additional fee(s)-including fees for net addition of claims-are required, beyond those that may otherwise be provided for in documents accompanying this paper. In the event, however, that an extension of time is necessary to allow consideration of this paper, such an extension is hereby petitioned under 37 C.F.R. §1.136(a). Any additional fees believed to be due in connection with this paper may be charged to our Deposit Account No. 09-0461.

Respectfully submitted,

Timothy J. O'Sullivan
Registration No. 35,632

Customer Number:

20792
PATENT TRADEMARK OFFICE

Certificate of Mailing under 37 CFR 1.8 (or 1.10)

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Non-Fee Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on July 17, 2003.

Traci A. Brown